Amendments to the Specification

Please replace the paragraph [0028] with the following amended paragraph:

"Techniques relevant to tamper-resistance are well known to those skilled in the art of security. These techniques include methods for resisting tampering (such as appropriate encapsulation of the trusted device), methods for detecting tampering (such as detection of out of specification voltages, X-rays, or loss of physical integrity in the trusted device casing), and methods for eliminating data when tampering is detected. ~~Further discussion of appropriate techniques can be found at http://www.cl.cam.ac.uk/~mgk25/tamper.html.~~ It will be appreciated that, although tamper-proofing is a most desirable feature of the present invention, it does not enter into the normal operation of the invention and, as such, is beyond the scope of the present invention and will not be described in any detail herein."

Please replace the paragraph [0066] with the following amended paragraph:

"Compartments 410, 460 will now be described further. A compartment 410, 460 is an environment containing a virtual computing engine 411, 461 wherein the actions or privileges of processes running on these virtual computing engines are restricted. Processes to be performed on the computing engine within a compartment will be performed with a high level of isolation from interference and prying by outside influences. Such processes are also performed with a high level of restriction on interference or prying by the process on inappropriate data. These properties are the result of the degree of reliability, because of the restrictions placed on the compartment, even though there is not the same degree of protection from outside influence that is provided by working in the trusted space 401. A well known form of compartment is a Java sandbox, in which case the virtual computing engine 411, 461 is a Java Virtual

Machine (JVM). Java Virtual Machines and the handling of security within Java are described at the Sun Microsystems Java web site ~~(http://java.sun.com, particularly http://java.sun.com/security)~~. To implement sandboxes, a Java platform relies on three major components: the class loader, the byte-code verifier, and the security manager. Each component plays a key role in maintaining the integrity of the system. Together, these components ensure that: only the correct classes are loaded; the classes are in the correct format; untrusted classes will not execute dangerous instructions; and untrusted classes are not allowed to access protected system resources. Each component is described further in, for example, the white paper entitled "Secure Computing with Java™.: Now and the Future" or in the Java Development Kit 1.1.X ~~(both obtainable from Sun Microsystems, for example at http://java.sun.com)~~. An example of the use of Java Virtual Machines in a compartmental environment is provided by HP Praesidium VirtualVault (basic details of HP Praesidium VirtualVault are described on HP's Internet site at ~~http://www.hp.com/security/products/virtualvault/papers/brief.sub.-4.0/)~~."